



WHITE PAPER

MANAGING PEER-TO-PEER TRAFFIC WITH CISCO SERVICE CONTROL TECHNOLOGY

Peer-to-peer (P2P) traffic consumes network resources without creating additional revenue. It is estimated that 70 percent or more of broadband bandwidth is consumed by downloads of music, games, video, and other content. Consumption will increase as P2P downloads multiply because of increases in subscriber adoption and file sizes. Identifying P2P applications is complex. Sophisticated P2P protocols can dynamically hop to different ports, making them difficult to detect, monitor, and control. Many existing devices and unsophisticated service control technologies lack the ability to detect changing P2P protocols, hampering a service provider's ability to address P2P application management. Cisco® Service Control with stateful deep packet inspection enables subscriber and application awareness, thereby helping ensure the identification, detection, and management of P2P.

SUMMARY

As P2P file-exchange applications gain popularity, Internet service providers (ISPs) are faced with added challenges when managing operational and capital expenses. Simultaneously, P2P offers operators opportunities to increase profitability from their broadband IP networks. Because of the aggressive consumption of network resources by P2P technologies, usage patterns are changing and current capacity provisioning schemes have not been optimized for “broadband-aware” traffic. Extensive use of P2P file exchange causes network congestion and performance deterioration, which can ultimately lead to customer dissatisfaction and turnover.

This paper discusses the unique problems associated with the growing popularity of P2P applications and how they affect the IP network; it offers various remedies that Cisco Service Control technology offers network operators. These include detailed usage accounting of P2P traffic as well as monitoring and billing, based on such information and the use of service control policies. The high level of data abstraction and presentation that the Cisco Service Control platform offers can help ISPs better manage these business challenges and avoid alienating their customer base by deploying proactive policies that are not perceived as intrusive or unfair by subscribers.

Internet P2P is a relatively new phenomenon, which allows for the creation of decentralized, dynamic, and anonymous logical networks for information exchange over the public Internet. As opposed to “traditional” client-server models, in which a well-known source provides content and information to requesting clients, P2P applications use various techniques to allow users to search and share information and content between themselves. These files often contain copyrighted material such as music, movies, software, etc.

P2P clients change frequently, and some are more popular in different geographies. For example, WinMX, because of Unicode support, is particularly popular in Japan and other parts of Asia. Other P2P protocols have followings based on the application content. Some of the more popular P2P protocols include the following:

- KaZaA
- Gnutella
- Winny
- WinMX
- eDonkey
- BitTorrent

- DirectConnect
- Manolito
- Kuro
- Soulseek
- Filetopia
- iTunes
- Napster
- Waste
- Mute
- Share

CHALLENGE

The popularity of P2P applications is causing significant concerns for the owners of copyrighted material, and it also creates network capacity and subscriber management problems for ISPs. Every IP network is built with usage assumptions, which, in turn, are used to analyze and compute network capacity and the resources needed to support a targeted subscriber base. This analysis is essential for service providers to sustain their return-on-investment (ROI) model. Because P2P applications differ from traditional client-server applications in the way they operate, they fall outside the parameters that existing network infrastructure is designed to meet.

Table 1 reviews some of the factors service providers consider when planning the network and demonstrates how P2P technologies can impact a provider's baseline assumptions.

Table 1. Factors ISPs Consider When Planning Networks

Parameter	Relevance to Network Planning	Traditional Application	P2P Impact
Upstream/downstream traffic ratio	The asymmetrical nature of networks mandates that the amount of upstream traffic the network sustains differs from the amount of downstream traffic. The ratio is correlated to application requirements. If the network ratio assumption is incorrect, congestion and unused capacity results.	Typical residential network use for applications such as e-mail, Web browsing, etc. generates a larger amount of downstream traffic for a single upstream request. Service providers tend to rely on this ratio.	With P2P applications, users share files and a typical peer serves megabytes of files, causing a shift in the upstream/downstream ratio. Congestion results on the upstream link because of a larger number of subscribers using the upstream link.
Time of day and percentage of activity	Based on subscriber profiling, service providers assume an average duration of network use per subscriber per day as well as peak-use periods. Typically service providers can predict and manage network "rush hours" as well as less-congested periods of network use. One important assumption is that residential home subscribers use the network primarily during weekends and at night, whereas telecommuters and small office or home office (SOHO) users are active during business hours. Sporadic changes in these patterns may cause unplanned congestion.	Time-of-day and percentage-of-activity assumptions for residential broadband subscribers assume the user is active only when present, typically weekends and evenings.	P2P applications run 24 hours in the background, constantly downloading content, and are left unattended for days at a time. Providers have not factored these applications into time-of-day policies.

Parameter	Relevance to Network Planning	Traditional Application	P2P Impact
Traffic destination and peering points	The cost associated with serving each network packet and connection can depend on the location of a subscriber's peer. Crafting peering agreements with other network providers reduces the amount of traffic and the cost of expensive transit connections. Local traffic (on-net) that does not leave the service provider's backbone network costs less than traffic leaving the provider's domain (off-net).	Traditional uses of the data network are mainly on-net (e-mail, Network News Transport Protocol [NNTP], or Web proxies) or destined for a small number of content providers and data sites.	P2P traffic significantly increases the amount of traffic between home users. Prior to P2P, direct connections between home users were rare. P2P file exchange increases direct connections, which can be on-net and off-net, increasing costs.
Estimated traffic volume	Network bandwidth is finite for all its users, and certain oversubscription assumptions are used when planning the capacity of the network.	Traditional applications have a large "time-to-consume" factor: A small Webpage can take several minutes to read, and a single e-mail message might take several hours to process.	P2P applications are mainly used to share large binary files that have a much lower "attention-per-byte" ratio. A typical music download occurs at 3- to 5-MB speeds, whereas a movie download is at GB speeds.

Individual network architecture and topology can determine how severely a service provider is impacted by P2P traffic. Common difficulties caused by the rise in P2P application usage can be the result of:

- Physical attributes of the shared cable infrastructure—Cable high-speed data (HSD) providers are particularly limited in the amount of upstream network resources they have; they need to go through a costly configuration process (fiber node splits) to expand the capacity. Because P2P applications cause a dramatic increase in upstream data, they pose both cost and maintenance challenges for cable HSD providers.
- P2P traffic traversing expensive network access points of regional service providers, such as those connecting their own IP network to the Internet over an international link (local file swapping between subscribers on the same network is less of a concern).

Service providers can no longer afford to ignore the increasing popularity of P2P. The impact of P2P applications on network traffic patterns, capacity planning, and infrastructure upgrades is significant. As P2P usage increases, so does network congestion, thereby decreasing performance for all users and applications.

When compared to dialup access or the competition, network speed has been a major selling point for broadband providers. To continue to grow their subscriber base of telecommuters and SOHO customers, service providers must offer assurances of predictable performance. The growth of P2P application usage threatens to challenge both a service provider's network design and service-level-agreement (SLA) assumptions.

SOLUTION

Cisco Systems® Service Control technology can help service providers manage and control bandwidth-hungry applications and address the challenges posed by aggressive P2P applications. P2P applications are designed to consume available bandwidth; therefore, a service provider that adds capacity is accommodating a perceived increase in demand that does not exist. The cost-to-revenue equation remains unbalanced because no additional revenue is received to offset the added costs of network management and expansion.

To avoid this situation, service providers must:

- Find out what P2P traffic is causing network congestion or increasing expenses and contain its effect
- Identify those subscribers who are consuming unrestricted amounts of network capacity
- Develop different subscription plans to compensate for the increased expense of carrying this type of network traffic

Simultaneously, service providers must ensure they do not alienate subscribers by changing subscription plans and implementing severely restrictive usage policies. Subscribers have become accustomed to unlimited use or flat-fee pricing models and need to be conditioned to accept revised business propositions. Service control offers providers a variety of options that can be effectively used to curb abuse, take advantage of existing network investment, and successfully manage high-bandwidth applications or provide incentives that offer subscribers a potential substitution when dealing with P2P applications.

Cisco Service Control offers granular usage analysis and helps enable providers to optimize traffic at the application level offering rich tools for the control and management of P2P traffic. Cisco Service Control can:

- Identify and classify all P2P traffic so that it can be accurately accounted for and controlled
- Enforce policies that address problems caused by the excessive P2P traffic without influencing other IP traffic or alienating subscribers

As simple as this may sound, these business goals are difficult to achieve with conventional means.

Identifying P2P Traffic

To understand the nature of the P2P traffic that is running on a network and to control its use, a service provider must first have a tool in place that can identify P2P-related packets and differentiate them from other IP traffic. However, many of the communication protocols used by P2P applications use different techniques than other communication protocols, making it extremely difficult to detect them using traditional techniques. Specifically, many P2P protocols do not use static, well-known port numbers, but rather dynamically use available port numbers and can frequently mask themselves by using ports reserved for other applications. For example, KaZaA uses port 80, typically reserved for HTTP Web browsing for its own communication, allowing it to penetrate firewalls and network packet filters. This makes it impossible to identify, track, or control P2P traffic by using simple port-based classification.

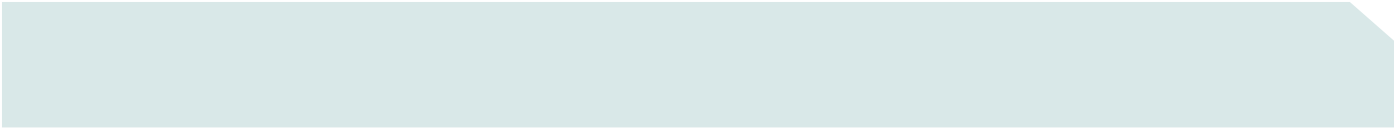
Moreover, the popularity of P2P applications is increasing. As new P2P applications come online they use different protocols, so any effective service control solution must be capable of detecting a new or emerging protocol—requiring the solution to be fully extensible and programmable. Any mechanism used to identify and classify P2P traffic must easily adapt to an ever-changing application environment.

Controlling P2P Traffic with Smart Policies

Policies that may be seen as too restrictive carry the risk of subscriber alienation, but “smart policies” can be enabled by using the granular analysis and control capabilities offered by an advanced service control solution. Some examples might include:

- Deprioritizing P2P during congestion periods
- Throttling upstream traffic (file upload) while not limiting downstream traffic (file downloads)
- Limiting P2P access during certain periods of the day or week (for example, business hours vs. weekends)
- Limiting P2P traffic traversing expensive peering points or transits
- Providing unrestricted subscription plans for an additional charge
- Enforcing a P2P quota, which when depleted throttles back P2P traffic but does not affect other application traffic
- Providing optional P2P “bandwidth on demand” for an additional charge

Existing quality-of-service (QoS), queuing, and shaping mechanisms are insufficient to implement these “smart policies” because they do not provide the required level of control. Furthermore, because existing infrastructure cannot identify P2P traffic, it cannot isolate and control P2P applications and distinguish it from other applications such as Web browsing, VPN, and e-mail.



Cisco Service Control technology enhances the existing transport network with subscriber and application awareness. By enabling the network to identify subscribers, classify applications, apply application-level traffic optimization, and charge for individual applications, providers can better manage and control high-volume use and profit from tailoring offerings to meet individual subscriber needs.

HOW A CISCO ADVANCED SERVICE CONTROL SOLUTION CAN HELP

Cisco Service Control technology is a state-of-the-art, dedicated network device, providing detection and control of P2P application usage and excessive bandwidth consumption. Using the Layer 7 stateful deep packet inspection capability of the platform, the solution can accurately identify P2P traffic and identify “abusive subscribers.” Furthermore, the advanced traffic management and control capabilities of the platform provide the means to contain and moderate excessive bandwidth usage, while preventing subscriber alienation. Providers are no longer forced to make binary decisions such as enforcing restrictive policies that might, for example, block P2P traffic, thereby alienating subscribers who want to take advantage of music and video download capabilities.

Stateful Deep Packet Inspection Capability

True service control solutions have a unique set of characteristics and architectural attributes that are designed to perform real-time traffic classification, accounting, and control. In order to undertake stateful deep packet inspection at multigigabit speeds, a purpose-built hardware architecture is required that is capable of maintaining the state of every network conversation, while executing deep and detailed inspection of every data packet through the application or Layer 7 network layer. The result is a solution that can detect specific P2P application signatures usually found during the initial message exchange between two network hosts and can classify all traffic for that conversation.

The Cisco Service Control platform generates usage statistics on every subscriber and for each application and protocol used. This allows service providers to identify “abusive subscribers” in real time. The usage information generated by the solution can be used to produce simple-to-understand, detailed reports on network activities, including:

- Top-volume consumers (identifying the most active subscribers)
- Detailed subscriber usage (outlining how the network was used by a particular subscriber), offering unsurpassed visibility into network activity and, therefore, a key to gaining insight on which subscribers are abusing the network, how they are doing it, and what the best control policies to moderate their use might be

This information is critical for both understanding the usage pattern in the network for all subscribers and potentially identifying those subscribers that are creating unacceptably high traffic volume.

Programmable for Real-Time Control

The Cisco Service Control platform protocol classification mechanisms are extremely flexible and programmable, facilitating rapid and reliable upgrades to classification of new codes in a fraction of the time it typically takes to upgrade a network device. This is important for the detection of P2P protocols, because these protocols change frequently with the release of new applications and new versions of existing ones.

Controlling P2P with Cisco Advanced Service Control

The proactive traffic control and bandwidth management capabilities of the Cisco Service Control platform provide a simple-to-use, yet highly effective means to relieve the strain caused by P2P traffic and abusive subscribers, while helping enable the creation of smart control policies to limit subscriber alienation. Granular analysis and application-level traffic optimization help ensure the ability to establish appropriate policies for dealing with P2P as well as virtually any IP application running on a provider's network. In the case of P2P, some examples of policy proliferation enabled by the Cisco Service Control solution include:

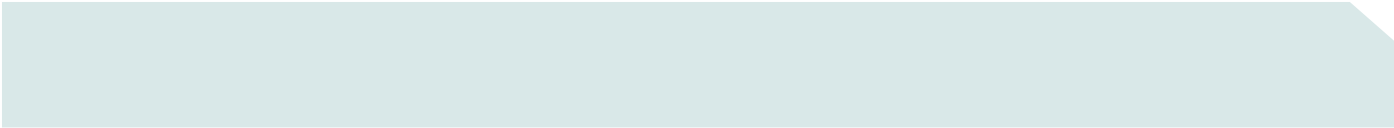
- *Aggregated rate limiting*—Limit all P2P traffic to a certain percentage of the available bandwidth. Although this does not provide fairness between subscribers, it can be used to eliminate the performance degradation caused by excessive P2P traffic on other network activities such as VPN, browsing, streaming, etc.
- *Upstream control limit*—Manage upstream P2P traffic (file uploads), while allowing downstream traffic (file downloads) to continue uninterrupted. This can provide relief to overcongested upstream links while not disrupting file downloads, thus posing less limitation on subscribers. The ability to isolate and control P2P uploads is essential to this policy because simply limiting upstream data would adversely influence all file transfer—uploads as well as downloads—by slowing down TCP connections.
- *Destination-based classification*—Limit traffic that uses expensive or particularly congested links, peering points, or transit connections, for example, expensive international links, thereby helping to reduce the cost associated with serving P2P traffic over expensive connections.
- *Time-of-day policies*—A Cisco Service Control platform can be configured to provide different limits on P2P usage during different periods of the day and week. This can be used to reduce the congestion caused by P2P traffic during those hours when other mission-critical and bandwidth-sensitive applications such as e-mail, VPN, etc. are used. Such policies also encourage P2P developers and users to automatically shift usage of the network to different hours of the day and week.
- *Subscriber application quotas*—Cisco Service Control technology can enforce a byte cap for a certain period of time, for example, a per-day quota, after which access can either be completely blocked or throttled to a minimum. The platform can enforce these quotas at the application level, meaning that the byte cap can be performed specifically on P2P traffic, offering subscribers the assurance that no matter how many P2P bytes have been consumed, they will not lose access to other critical applications, for example, VPN, e-mail, etc.
- *Subscriber dynamic policies*—Taking advantage of Cisco Service Control subscriber awareness, dynamic policies can be implemented to allow subscribers to control their own accounts. For example, the service provider can design a subscription package that provides unlimited P2P access for an additional charge or develop a “bandwidth-on-demand” system whereby a subscriber can buy additional bandwidth as needed. Such an offering gives subscribers the opportunity to manage their own accounts and can potentially open additional revenue streams for the service provider.

CONCLUSION

A P2P subscriber's aggressive use of network resources coupled with the growing popularity of P2P applications puts significant strain on a provider's broadband network. Service providers must find ways to manage high-bandwidth users that maintain customer satisfaction as well as the overall subscriber user experience. By avoiding costly capacity upgrades and fiber node splits, Cisco Service Control technology is an ideal, cost-effective means to address the P2P problem while simultaneously developing a new business opportunity.

The primary capabilities of the platform follow:

- Tracking the state of each network connection and performing application or Layer 7 traffic analysis helps enable reliable and accurate classifying of traffic such as P2P.
- A programmable architecture capable of rapidly addressing new protocols and applications keeps a service provider up-to-date with the dynamic state of P2P applications and protocols.

- 
- Cisco Service Control offers the ability to track traffic flows at multimegabit speeds, thereby providing unsurpassed performance while executing the most complex policies.
 - Cisco Service Control provides a transparent network overlay that requires minimal network reconfiguration while maintaining the investment in existing network equipment and infrastructure.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R) De/LW7904 02/05

